UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/559,767	03/16/2006	Roberto Avanzi	DE030202US1	5670

65913 7590 11/25/2009

NXP, B.V.
NXP INTELLECTUAL PROPERTY & LICENSING
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
GELAGAY, SHEWAYE	

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
11/25/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	**Application No.** 10/559,767	**Applicant(s)** AVANZI, ROBERTO
	Examiner SHEWAYE GELAGAY	**Art Unit** 2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 July 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the Applicant's amendment filed on July 16, 2009.

2. Claims 1-10 have been amended. New claims 11-13 are added. Claims 1-13 are pending.

Response to Arguments

3. Applicant's arguments filed on July 16, 2009 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-4, 7-8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coron et al., "Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems" 1999, pages 1-11 (hereinafter Coron) in view of Lauter et al. (hereinafter Lauter) US 7,043,015.

2. As per claims 1, 7-8 and 10:

Coron teaches a method for defence against at least one attack made by means of differential power analysis, the method comprising:

randomizing at least one factor in a elliptic public key cryptosystem, which is given by at least one hyperelliptic curve of any genus over a finite field in a first group, where the hyperelliptic curve is given by at least one coefficient, wherein the factor is selected from the group consisting of: the hyperelliptic curve; and at least one element of the first group, in particular at least one in particular reduced divisor and/or at least one intermediate result of a scalar multiplication is randomised. (*5. Countermeasures Against DPA; introducing random numbers during the computation of Q=dP; 5.3 randomized projective coordinates...randomizing the projective coordinate representation of a point P=(X,Y,Z). Before each new execution of the scalar multiplication algorithm for computing Q=dP, the projective coordinates of P are randomized according to equation (3) with a random λ. The randomization can also occur after each point addition and doubling*)

Coron does not explicitly disclose a hyperelliptic public cryptosystem. Lauter in analogous art, however, discloses a hyperelliptic public cryptosystem. (col. 4, line 1-col. 5, line 18) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Coron with Lauter in order to provide advantage of improved security while requiring shorter key lengths. (col. 2, lines 15-35; Lauter)

As per claim 2:

The combination of Coron and Lauter teaches all the subject matter as discussed above. In addition, Coron further teaches wherein bits of the operand to be processed or encoded in the hyperelliptic public key cryptosystem are represented by t least one co-efficient of the hyperelliptic curve. (5. *Countermeasures Against DPA; introducing random numbers during the computation of Q=dP; 5.3 randomized projective coordinates. Before each new execution of the scalar multiplication algorithm for computing Q=dP, the projective coordinates of P are randomized according to equation (3) with a random λ. The randomization can also occur after each point addition and doubling*)

As per claim 3:

The combination of Coron and Lauter teaches all the subject matter as discussed above. In addition, Coron further teaches that at least one scalar multiplication in the Jacobian variation of the hyperelliptic curve takes place in a second group different from the first group and isomorphic in relation to the first group, in particular selected at random. (*pages 11-14; A.1 Elliptic curves over a field K with Char K!= 2,3 ... With their coordinates, called modified Jacobian coordinates, a point (X: Y: Z) is internally represented as a 4-tuple (X,Y,Z,aZ4)*)

As per claim 4:

The combination of Coron and Lauter teaches all the subject matter as discussed above. In addition, Coron further teaches the following steps:

transforming of the Jacobian variation of the hyperelliptic curve by means of at least one K-isomorphism, into the Jacobian variation of the transformed hyperelliptic curve; (*pages 11-14; A.1 Elliptic curves over a field K with Char K!= 2,3 ... With their coordinates, called modified Jacobian coordinates, a point (X: Y: Z) is internally represented as a 4-tuple (X,Y,Z,aZ4)*) multiplying of the Jacobian variation of the transformed hyperelliptic curve with at least one scalar; (*pages 11-14; A.1 Elliptic curves over a field K with Char K!= 2,3 ... With their coordinates, called modified Jacobian coordinates, a point (X: Y: Z) is internally represented as a 4-tuple (X,Y,Z,aZ4)*) and

transforming of the Jacobian variation multiplied by the scalar of the transformed hyperelliptic curve by means of the depiction inverse to the depiction in a Jacobian variations of the hyperelliptic curve multiplied by scalars, where the depiction corresponds to the transition from the first group to the second group and the inverse depiction corresponds to the transition from the second group to the first group. (*pages 11-14; A.1 Elliptic curves over a field K with Char K!= 2,3 ... With their coordinates, called modified Jacobian coordinates, a point (X: Y: Z) is internally represented as a 4-tuple (X,Y,Z,aZ4)*)

3. Claims 5-6 and 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Coron et al., "Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems" 1999, pages 1-11 (hereinafter Coron) in view of Lauter et al. (hereinafter Lauter) US 7,043,015 and in view of Lange "Weighted Coordinates on Genus 2 Hyperelliptic Curves" October 11, 2002, pages 1-20.

As per claim 5:

The combination of Coron and Lauter teaches all the subject matter as discussed above. Both references do not explicitly disclose the steps: depictiing of at least one reduced divisor with an associated polynomial pair as at least one quintuplet in projective co-ordinates, where U(t)=t.sup.2+U.sub.1t/Z+U.sub.0/Z and

V(t)=V.sub.1t/Z+V.sub.0/Z; randomly selecting at least one non-vanishing element from the field; and conversion of the quintuplet by means of a selected element into the converted quintuplet. Lange in analogous art, however, further discloses the steps: depiction of at least one in particular reduced divisor with associated polynomial pair as at least one quintuplet in projective co-ordinates, where (t)=t.sup.2+U.sub.1t/Z+U.sub.0/Z and V(t)=V.sub.1t/Z+V.sub.0/Z; randomly selecting of at least one non-vanishing element from the field; and conversion of the quintuplet by means of a selected element into the converted quintuplet. (*pages 2-3; 2. The New System of Coordinates; coordinates one lets [U1U0V1V0Z stand for X^2+U1/Zx+U0/Z and V1/Zx+V0/Z*) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Coron and Lauter with Lange in order to obtain inversion free formulae that are faster than projective by considering weighted coordinates. (Abstract; Lange)

As per claim 6:

The combination of Coron and Lauter teaches all the subject matter as discussed above. Coron does not explicitly disclose the following steps: depicting at least one reduced divisor with associated polynomial pair as at least one sextuplet a projective co-ordinates, where U(t)=t.sup.2+U.sub.1t/Z.sub.1.sup.2+U.sub.0/Z.sub.1.sup.2 and V(t)=V.sub.1t/(Z.sub.1.sup.3Z.sup.2)+V.sub.0/(Z.sub.1.sup.3Z.sub.2); randomly selecting at least two non-vanishing elements from the field; and converting the sextuplet by means of a selected elements into the converted sextuple. Lange in analogous art, however, further discloses the following steps: depicting at least one in particular reduced divisor with associated polynomial pair as at least one sextuplet a projective co-ordinates, where U(t)=t.sup.2+U.sub.1t/Z.sub.1.sup.2+U.sub.0/Z.sub.1.sup.2 and V(t)=V.sub.1t/(Z.sub.1.sup.3Z.sup.2)+V.sub.0/(Z.sub.1.sup.3Z.sub.2); randomly selecting of at least two non-vanishing elements from the field; and conversion of the sextuplet by means of a selected elements into the converted sextuple. (*pages 2-3; 2. The New System of Coordinates; let [U1,U0,V1,V0,Z1,Z2] correspond to affine point [X^2+U1/Z^2x+u0/z^21, V1/z^3Z2x+V0/Z^3iZ2]*) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Coron and Lauter with Lange in order to obtain inversion free formulae that are faster than projective by considering weighted coordinates. (Abstract; Lange)

As per claim 11:

The combination of Coron and Lauter teaches all the subject matter as discussed above. Both references do not explicitly disclose wherein randomizing at least one element of the firs group comprises randomizing at least one reduced divisor. Lange in analogous art, however wherein randomizing at least one element of the firs group comprises randomizing at least one reduced divisor. (*pages 2-3*) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Coron and Lauter with Lange in order to obtain inversion free formulae that are faster than projective by considering weighted coordinates. (Abstract; Lange)

As per claim 12:

The combination of Coron and Lauter teaches all the subject matter as discussed above. Both references do not explicitly disclose wherein randomizing at least one element of the firs group comprises randomizing at least one intermediate result of scalar multiplication. Lange in analogous art, however, wherein randomizing at least one element of the firs group comprises randomizing at least one intermediate result of scalar multiplication. (*pages 2-3*) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Coron and Lauter with Lange in order to obtain inversion free formulae that are faster than projective by considering weighted coordinates. (Abstract; Lange)

As per clam 13:

The combination of Coron and Lauter teaches all the subject matter as discussed above. Both references do not explicitly disclose wherein bits of the operand to be processes and/or encoded in the hyperelliptic public key cryptosystems are represented by at least one base element of the cryptosystem, wherein the base element comprises at least one reduced divisor, at least one intermediate result of a scalar multiplication, or at least one of each of the reduced devisor and the intermediate result of the scalar multiplication. Lange in analogous art, however, wherein bits of the operand to be processes and/or encoded in the hyperelliptic public key cryptosystems are represented by at least one base element of the cryptosystem, wherein the base element comprises at least one reduced divisor, at least one intermediate result of a scalar multiplication, or at least one of each of the reduced devisor and the intermediate result of the scalar multiplication. (*pages 2-3*) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Coron and Lauter with Lange in order to obtain inversion free formulae that are faster than projective by considering weighted coordinates. (Abstract; Lange)

4. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over by Coron et al., "Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems" 1999, pages 1-11 (hereinafter Coron) in view of Lauter et al. (hereinafter Lauter) US 7,043,015 and in view of Okeya et al. (hereinafter Okeya) US 2003/0059042.

As per claim 9:

a. The combination of Coron and Lauter teaches all the subject matter as discussed above. Both references do not explicitly disclose a device a smart card, with at least one microprocessor as claimed in claim 8. Okeya in analogous art, however, discloses a device a smart card, with at least one microprocessor as claimed in claim 8. (*figure 6, item 701; paragraph [164-170]*) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Coron and Lauter with Okeya in order to safeguard against side channel attack and further carry out the processing at high speed. (paragraph [187]; Okeya)

5. Claims 1 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Joye et al., "Protections against Differential Analysis for Elliptic Curve Cryptography" Springer-Verlag, 2001, pages 1-15 (hereinafter Joyce) in view of Lauter et al. (hereinafter Lauter) US 7,043,015.

As per claims 1 and 8:

Joyce teaches a method for defence against at least one attack made by means of differential power analysis in at least one hyperelliptic cryptosystem, in particular in at least one hyperelliptic public key cryptosystem, which is given by at least one hyperelliptic curve of any genus over a finite field in a first group, where the hyperelliptic curve is given by at least one coefficient, characterised in that the hyperelliptic curve and/or at least one element of the first group, in particular at least one in particular reduced divisor and/or at least one intermediate result of a scalar multiplication is randomised. (*4. Randomizing the Basepoint*)

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHEWAYE GELAGAY whose telephone number is (571)272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. G./
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437